C. Hoare & Co.

PRIVATE BANKERS SINCE 1672

Staying Safe from Fraud

Staying Safe from Fraud

The UK banking industry has worked hard to protect customers from the threat of fraud. However, that threat is rising. Fraudsters are endlessly inventive and they are skilled at finding weak spots in defences. They exploit any opportunity - from an unprotected password to a global health crisis - to steal money and disrupt lives.

Your safety is our priority. Our Fraud team is constantly alert to new scams and malpractice and we want to help our customers stay vigilant, too. In this guide you will find advice on how to spot and avoid the most common scams. Please take time to read the information carefully. If you have any questions or concerns, the Fraud team will be happy to hear from you by telephone (020 7353 4522) or by email (**CustomerFraudSupport@hoaresbank.co.uk**).

Similarly, if you believe you have been the victim of fraud, please let the bank know immediately. Day or night, there will be someone to help.

Contents

Common Frauds and Scams

Fraudsters are skilled in the art of psychological manipulation. They will do everything in their power to persuade you to divulge confidential information or to perform actions that are not in your best interest. This kind of scam is known as 'social-engineering fraud' and takes many forms. The aim, however, is always to steal money or valuable data.

Here are some of the ways criminals may try to defraud you:

Impersonation Fraud

The fraudster may claim to represent an organisation you trust; this could include C. Hoare & Co., a utility company, a telephone/internet service provider, a government department (most commonly HMRC), or the police. Impersonation scams can be carried out by telephone, text or email.

Criminals can be very persuasive and may put you under pressure to act immediately. ('If you don't do this right now, your account will be emptied/ your service will be cut off/ you risk a penalty.') They may also use a tactic called 'spoofing' to make their message look genuine by cloning the number or sender ID of legitimate organisations.

Telephone fraud ('vishing')

The caller purports to be telephoning from a trusted organisation and demands confidential information relating to an account you hold with them. They may demand payment over the phone or they may say the security of your account has been compromised/ breached by a fraudster and ask you to move money to a 'safe account' as a matter of urgency.

Text fraud ('smishing')

A fraudster may also try to trick you into giving them valuable personal information via a text message. Smishing texts generally ask you to click on a link and enter your personal details, or they may ask you to telephone an organisation you know and trust on a specified number. As well as harvesting your personal information, websites you visit via smishing texts can infect your internet-connected phone with malware.

Alternatively, a smishing text may ask you to telephone a trusted organisation on a specified number, enabling the fraudster to listen in to your call, or the call may in fact be to a premium-rate number, resulting in exorbitant charges being added to your phone bill.

Email fraud ('phishing')

Emails purporting to be from reputable organisations may induce you to reveal personal information such as bank account details and passwords. These emails may mimic the communications style of companies you are used to dealing with, using logos, typefaces and layouts familiar to you.

Typically, fraudsters will send an unsolicited email containing an attachment or link to another website. When you click on the attachment or link as requested, you will either be directed to a fake website or you will, without any noticeable permission request, allow malware to be downloaded onto your device.

How to protect yourself

- Always question why a trusted organisation would contact you in this way. Remember neither C. Hoare & Co. nor any reputable company will ever contact you out of the blue, asking for payment or for confidential information.

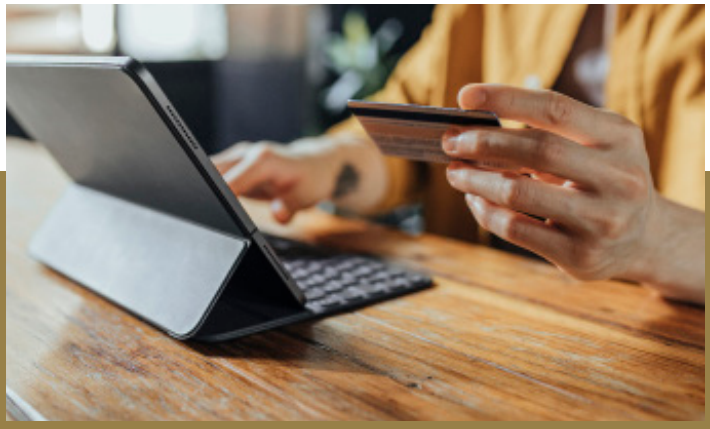
  If in doubt, call the organisation on a number already known to you to check the authenticity of the message and do not click on links unless you are 100% satisfied.

- You should be suspicious of messages that:
  - use a generic greeting ('Hello', 'Hi there,' etc.) instead of your name and title
  - say your account is on hold because of a billing problem
  - ask you to 'validate' your account
  - invite you to click on a link to update your payment details
  - say you are due a tax refund from HMRC
  - offer free gifts

- Please treat as suspicious any offer of goods or services that seems too good to be true and do not respond to the message (even if you haven't clicked a link). If you engage with the fraudster in any way, you may be added to a list of likely dupes and inundated with similar messages.

NB Some scammers are exceptionally plausible. If they play on your sympathy/anxiety, and you find it difficult to say 'No' outright, tell them you do not have authority to do as they ask or explain that you need time to verify the request. If they are a genuine professional, they will understand why you are checking; if they become pushy or insistent, they are almost certainly criminals.

Online Shopping Fraud



Fraudsters have been quick to capitalise on the increased popularity of online shopping. While many sellers are legitimate, fake websites abound; these may look almost identical to genuine online retailers, with professional layouts and stolen logos. However, items bought from such sites are likely to be cheap fakes (possibly dangerous in the case of electronics) and often you will receive nothing at all.

How to protect yourself

- Wherever possible, buy goods from trusted brands or stores that are known to you. When luxury goods are offered at very low prices, you should be suspicious. If a bargain looks too good to be true, it probably is!
- Watch out for poor English, with mistakes in spelling or grammar, as this often indicates a scam run from overseas.
- Please take extra care when paying for goods and services by bank transfer: scammers prefer this method as, once the transaction has been completed, there is very little you can do to get your money back. Paying by credit card will help you stay safe and provide protection for your purchases.
- Some retailer websites/apps will request confirmation of a One-Time Passcode as an extra layer of payment protection. Please remember this code should never be shared with anyone, even if they claim to be calling from the bank.
- Look for the padlock symbol: a secure site is indicated by a padlock displayed next to the company name in the address bar. If you do not see the padlock, please take extra care when making a payment.
- Always check the name in the address bar matches exactly the name of the company you wish to buy from, in case you have been redirected to a fraudulent website. (Legitimate online sellers are unlikely to have domain names ending in .net or .org.)
- Genuine online retailers should display a ‘shipping and returns’ policy. If there is no published mechanism for returning faulty goods, you should be suspicious.
- Check your bank account on a regular basis; review your transactions via online banking, the mobile app or your monthly statement. If you find a transaction you don’t recognise, please contact the bank immediately.

Workplace Fraud

Electronic communications in the workplace and the rise of the 'virtual office' present lucrative opportunities for fraudsters.

CEO fraud occurs when a criminal pretending to be a CEO or senior member of staff sends a payment instruction, typically via email, to a finance department or personal assistant. The scam relies on the assumption that, given the seniority of the supposed sender, the payment will not be challenged; this can result in very substantial financial losses. While 'spoofed' emails are common in this type of scam, fraudsters have been successful even where email accounts have not been compromised: they simply create an email account name that closely resembles the real thing.

Small businesses are also at risk. Personal assistants or family offices may act on instructions they believe have come from their employer but that are in reality from fraudsters.

Invoice and mandate fraud occurs when a criminal poses as a regular supplier and persuades you to change the bank account details you hold on file for that company. Payment is then redirected straight to the account of the scammer.

Fraudsters will carry out extensive research on your business to find out who your suppliers are and when payments are due. They may then intercept your email, gain access to your supplier's email account, or use a cloned email to facilitate the scam.

How to protect yourself

- Always double-check email addresses when making or approving payments. If in doubt, request verification by telephone or via an email address you know to be genuine.
- Any request to change the bank details of an existing supplier should be treated as suspicious. Do not reply to the email and verify the request by speaking to a known individual at the organisation in question.
- Regularly review internal procedures for requesting, approving and verifying transactions.

Bank Card Fraud

As cash transactions have become less frequent, card fraud has increased. Scammers are inventive and change their methods regularly. Criminals may fit devices to ATMs which clone your card ('skimming') or retain it within a cash machine; once you have left the scene, they will retrieve the cloning device or your card and use the information to make fraudulent purchases or steal your identity. Hand-held skimming devices may also be used in shops or restaurants.

Alternatively, criminals may use simple distraction techniques to steal your card or PIN. They may engage you in conversation while an accomplice steals your card or cash or divert your attention by dropping cash on the ground and asking if it is yours.

How to protect yourself

- Always shield your PIN when you are entering it into a cash machine.
- Never engage in conversation with another person while you are using an ATM.
- Never make card payments on a stranger's behalf (e.g. at parking-ticket machines).
- Check ATMs for signs of tampering (loose or blocked card slot/ bulky or 'spongy' pin pad/ misaligned or badly printed stickers). If you are in any doubt, use another machine.
- If your credit or debit card statements show purchases you do not remember making, or if your card provider lets you know you have exceeded your limit when you should have funds available, you should contact the bank or your card provider immediately.
- Please check card and bank statements regularly for suspicious transactions; the faster criminal activity is picked up, the easier it is to remedy.

Money Laundering Fraud

Criminals frequently move the proceeds of crime through the accounts of unrelated individuals to make the money appear ‘clean’. This is the Criminal Offence of Money Laundering under the Proceeds of Crime Act 2002. Anyone who allows criminal funds to pass through their bank account, or who allows their bank account to be used by an unauthorised person, is termed a ‘mule’ and is in breach of the terms of their bank account. Moreover, they may be prosecuted under the Proceeds of Crime Act and face a term of up to 14 years in prison.

Fraudsters may post on social media or on online jobs boards, advertising ‘easy cash schemes’, ‘flips’, or ‘money transfer jobs’. They may also strike up a relationship with their victims on online dating sites. At some point the victim will be asked to share their bank details so that cash can be deposited into their account, with instructions to send it on to another account, possibly in another country.

How to protect yourself

- Never give your financial details to someone you don’t know and trust. No legitimate company will ever ask you to use your personal bank account to transfer their money.
- Do not accept job offers from anyone who asks you to transfer money in return for a ‘fee’. It is always advisable to research potential employers carefully, particularly those based overseas.

How to report a fraud

If you believe you have been targeted or if you have fallen victim to a scam, as well as calling the bank, you can report the scam directly to Action Fraud on **0300 123 2040.**

Action Fraud is the UK's national reporting centre for fraud and cybercrime. Its website (**www.actionfraud.police.uk**) contains information and advice together with details of the latest fraud trends.

If you are worried your personal details have been stolen, you may wish to subscribe to the Cifas Protective Registration service. It will place a flag alongside your name and personal details in its secure National Fraud Database. Companies and organisations who are signed up as members of the database will see you're at risk and take extra steps to protect you and prevent fraudsters from using your details to apply for products and services.

For more information on the Cifas Protective Registration service please visit **www.cifas.org.uk** or telephone **0330 100 0180**.

Take Five

C. Hoare & Co. supports the Take Five campaign. This a national campaign, led by UK Finance and backed by Her Majesty's government, that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

Take Five advises extreme caution in any situation where you are sharing personal or banking details. You should make sure you are confident that the organisation you share your information with are who they say they are. A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account.

If you don't know who you are talking to, or there is reason to suspect that the provider is not who they claim to be, do not disclose your banking security details, or other personal or financial information.

Take Five urges you to stop and consider whether the situation is genuine – to stop and think if what you're being told really makes sense.

1. Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

2. Challenge: Could it be fake? Don't be afraid to reject, refuse or ignore requests. Only criminals will try to rush or panic you.

3. Protect: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

For more information on the Take Five campaign, please go to its website: **takefive-stopfraud.org.uk**